ON THE NUMBER OF POINTS OF SOME KUMMER CURVES OVER FINITE FIELDS

FLORIN NICOLAE

Let l be a prime number and let $k = \mathbb{F}_q$ be a finite field of characteristic $p \neq l$ with $q = p^f$ elements. Let $n \geq 1$. The curve

$$C_n : y^l = x(x^{l^n} - 1)$$

is smooth of genus $g_n = \frac{\varphi(l^{n+1})}{2} = \frac{l^n(l-1)}{2}$ over k. Let F_n/k be the function field of C_n, let $\mathbb{P}_{F_n}$ denote the set of places, and let $\mathrm{Div} F_n$ denote the group of divisors of F_n/k. The absolute norm $\mathfrak{N}(\mathfrak{P})$ of a place $\mathfrak{P} \in \mathbb{P}_{F_n}$ is the cardinality of its residue class field. It holds $\mathfrak{N}(\mathfrak{P}) = q^{\deg \mathfrak{P}}$, with a natural number $\deg \mathfrak{P} \geq 1$, the degree of $\mathfrak{P}$. The Zeta function of the curve C_n is a meromorphic function in the complex plane, defined for $\mathrm{Re}\, s > 1$ by

$$\zeta_{C_n}(s) = \prod_{\mathfrak{P} \in \mathbb{P}_{F_n}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{P})^s}} = \sum_{\mathfrak{A} \in \mathrm{Div} F_n,\, \mathfrak{A} \geq 0} \frac{1}{\mathfrak{N}(\mathfrak{A})^s}.$$

Denoting for $m \geq 0$ by A_m the number of positive divisors of degree m it holds

$$\zeta_{C_n}(s) = \sum_{m=0}^{\infty} \frac{A_m}{q^{ms}}.$$

The power series

$$Z_{C_n}(t) := \sum_{m=0}^{\infty} A_m t^m$$

is convergent for $|t| < q^{-1}$ and represents a rational function

$$Z_{C_n}(t) = \frac{L_{C_n}(t)}{(1-t)(1-qt)},$$

where $L_{C_n}(t) = q^{g_n} t^{2g_n} + \ldots + 1$ is a polynomial with coefficients in $\mathbb{Z}$ of degree $2g_n$. For $r \geq 1$ let N_r be the number of $\mathbb{F}_{q^r}$-rational points of the projective closure of C_n. Since the plane curve C_n has only one point $(0 : 1 : 0)$ at infinity, it holds

$$N_1 = N + 1$$

where N is the number of solutions (x, y) in k of the equation

$$y^l = x(x^{l^n} - 1).$$

Let $|X|$ denote the number of elements of a finite set X.

Lemma 1. *If $B(x) \in k[x]$ is a polynomial with a simple root $x_1 \in k$:*

$$B(x) = (x - x_1)B_1(x), B_1(x) \in k[x], B_1(x_1) \neq 0,$$

Date: November 13, 2005.

then the number of solutions in k of the equation

$$y^l = B(x)$$

is

$$N = \frac{1}{l}\sum_{j=0}^{l-1} |\mathcal{A}_j|,$$

where for $0 \leq j \leq l-1$

$$\mathcal{A}_j := \{(x,y) \in k \times k \mid y^l = \xi^j B_1(\xi^j x^l + x_1)\},$$

ξ *a generator of the cyclic multiplicative group* k^**.*

P r o o f: I) The case $q \equiv 1(\mod l)$. Let χ be a character of k^* of order l such that

$$\chi(\xi) = \omega = e^{\frac{2\pi i}{l}}.$$

Put $\chi(0) := 0$. It holds

$$N = q + \sum_{r=1}^{l-1}\sum_{c\in k}\chi^r(B(c)) = q + \sum_{r=1}^{l-1}\sum_{c\in k}\chi^r((c-x_1)B_1(c)) =$$

$$= q + \sum_{r=1}^{l-1}\sum_{c\in k}\chi^r(c-x_1)\chi^r(B_1(c)) =$$

$$= q + \sum_{r=1}^{l-1}\sum_{0\leq i,j\leq l-1}\sum_{c\in A, \chi^r(c-x_1)=\omega^i, \chi^r(B_1(c))=\omega^j}\omega^{i+j} =$$

$$= q + \sum_{r=1}^{l-1}\sum_{s=0}^{l-1}\omega^s \cdot \sum_{0\leq i,j\leq l-1,\, i+j\equiv s(\mod l)} |A_{i,j}^{(r)}|,$$

where

$$A := \{c \in k \mid B(c) \neq 0\},\ A_{i,j}^{(r)} = \{c \in A \mid \chi^r(c-x_1) = \omega^i, \chi^r(B_1(c)) = \omega^j\}.$$

For $1 \leq r \leq l-1$ let r^{-1} denote the representative in $1,\ldots,l-1$ of the class $\hat{r}^{-1}$ in the multiplicative group of non-zero residues modulo l. It holds

$$A_{i,j}^{(r)} = A_{r^{-1}i,r^{-1}j}^{(1)}$$

hence

$$\sum_{r=1}^{l-1}\sum_{s=0}^{l-1}\omega^s \cdot \sum_{0\leq i,j\leq l-1,\, i+j\equiv s(\mod l)} |A_{i,j}^{(r)}| = \sum_{r=1}^{l-1}\sum_{s=0}^{l-1}\omega^s \cdot \sum_{i=0}^{l-1}|A_{r^{-1}i,r^{-1}(s-i)}^{(1)}| =$$

$$= \sum_{r=1}^{l-1}\sum_{s=0}^{l-1}\omega^s \cdot \sum_{j=0}^{l-1}|A_{j,r^{-1}s-j}^{(1)}| = \sum_{r=1}^{l-1}\sum_{j=0}^{l-1}\sum_{s=0}^{l-1}\omega^s|A_{j,r^{-1}s-j}^{(1)}| =$$

$$= \sum_{r=1}^{l-1}\sum_{j=0}^{l-1}\sum_{t=0}^{l-1}\omega^{rt}|A_{j,t-j}^{(1)}| = \sum_{t=0}^{l-1}(\sum_{r=1}^{l-1}\omega^{rt})\sum_{j=0}^{l-1}|A_{j,t-j}^{(1)}| =$$

$$= (l-1)\sum_{j=0}^{l-1}|A_{j,l-j}^{(1)}| + \sum_{t=1}^{l-1}(-1)\sum_{j=0}^{l-1}|A_{j,t-j}^{(1)}| =$$

$$= l\sum_{j=0}^{l-1}|A_{j,l-j}^{(1)}| - \sum_{i,j=0}^{l-1}|A_{i,j}^{(1)}| = l\sum_{j=0}^{l-1}|A_{j,l-j}^{(1)}| - |A|,$$

so

$$N = q + l\sum_{j=0}^{l-1}|A_{j,l-j}^{(1)}| - |A|.$$

For $0 \le j \le l-1$ it holds

$$A_{j,l-j}^{(1)} = \{c \in A \mid \chi(c-x_1) = \omega^j, \chi(B_1(c)) = \omega^{l-j}\} =$$
$$= \{c \in A \mid \exists (t,u) \in k^* \times k^* : c - x_1 = \xi^j t^l,\ B_1(c) = \xi^{l-j}u^l\}.$$

Let

$$A_j := \{(t,u) \in k \times k \mid B_1(\xi^j t^l + x_1) = \xi^{l-j}u^l\},$$
$$B_j := \{(0,u) \mid \xi^{l-j}u^l = B_1(x_1)\} \cup \{(t,0) \mid B_1(\xi^j t^l + x_1) = 0\},$$

$0 \le j \le l-1$. Let $\rho \in k^* \setminus \{1\}$ with $\rho^l = 1$. For $0 \le j \le l-1$ the map

$$g_j : A_j \setminus B_j \to A_{j,l-j}^{(1)},$$
$$g_j(t,u) := \xi^j t^l + x_1$$

is surjective with the fibers

$$g_j^{-1}(c) = \{(\rho^d t, \rho^e u) \mid 0 \le d, e \le l\}$$

for $c \in A_{j,l-j}^{(1)}$ and fixed $(t,u) \in A_j \setminus B_j$ such that $g_j(t,u) = c$ consisting of l^2 elements. Therefore

$$|A_{j,l-j}^{(1)}| = \frac{1}{l^2}|A_j| - \frac{1}{l^2}|B_j| =$$
$$= \frac{1}{l^2}|A_j| - \frac{1}{l^2}|\{c \in k \mid \xi^{l-j}c^l = B_1(x_1)\}| - \frac{1}{l^2}|\{c \in k \mid B_1(\xi^j c^l + x_1) = 0\}|,$$

and so

$$l\sum_{j=0}^{l-1}|A_{j,l-j}^{(1)}| = \frac{1}{l}\sum_{j=0}^{l-1}|A_j| - \frac{1}{l}\sum_{j=0}^{l-1}|\{c \in k \mid \xi^{l-j}c^l = B_1(x_1)\}| -$$
$$-\frac{1}{l}\sum_{j=0}^{l-1}|\{c \in k \mid B_1(\xi^j c^l + x_1) = 0\}| =$$
$$= \frac{1}{l}\sum_{j=0}^{l-1}|A_j| - 1 - |\{d \in k \mid B_1(d) = 0\}|.$$

Since

$$k = A \cup \{c \in k \mid B(c) = 0\} = A \cup \{c \in k \mid B_1(c) = 0\} \cup \{x_1\}$$

it follows that

$$N = q + l\sum_{j=0}^{l-1}|A_{j,l-j}^{(1)}| - |A| =$$
$$= q + \frac{1}{l}\sum_{j=0}^{l-1}|A_j| - 1 - |\{d \in k \mid B_1(d) = 0\}| - |A| =$$
$$= \frac{1}{l}\sum_{j=0}^{l-1}|A_j| = \frac{1}{l}\sum_{j=0}^{l-1}|\mathcal{A}_j|,$$

because the map

$$\mathcal{A}_j \to A_j,\ (x,y) \mapsto (x, \xi^{-1}y)$$

is bijective.

II) The case $q \not\equiv 1(\bmod l)$. Each element of k has one and only one l-th root in k. It holds

$$N = q,\ |\mathcal{A}_j| = q,\ 0 \le j \le l-1. \square$$

For a character φ of the multiplicative group k^* let

$$\tau(\varphi) := -\sum_{c\in k^*} \varphi(c)\exp(\frac{2\pi i}{p}\mathrm{Tr}_{k/\mathbb{F}_p} c)$$

be the corresponding Gauss sum. For two characters φ_1 and φ_2 of k^* let

$$\iota(\varphi_1, \varphi_2) := -\sum_{c\in k} \varphi_1(c)\varphi_2(1-c)$$

be the corresponding Jacobi sum. If $\varphi_1 \cdot \varphi_2 \neq 1$ then

$$\iota(\varphi_1,\varphi_2) = \frac{\tau(\varphi_1)\tau(\varphi_2)}{\tau(\varphi_1\varphi_2)}. \tag{1}$$

For each natural number $m \ge 1$ let $\zeta_m := \exp\frac{2\pi i}{m}$ and let $\mu_m := \{\zeta_m^j \mid 0 \le j \le m-1\}$ be the group of complex m-th roots of unity.

Proposition 1. *a) If $q \not\equiv 1(\bmod l)$ then $N_1 = q+1$.*
b) If $q \equiv 1(\bmod l^{n+1})$ then

$$N_1 = q + 1 - \mathrm{Tr}_{\mathbb{Q}(\zeta_{l^{n+1}})/\mathbb{Q}}(\eta_n),$$

where

$$\eta_n := \iota(\psi^{l^n}, \psi),$$

ψ a character of k^* of order l^{n+1}.

P r o o f: a) If $q \not\equiv 1(\bmod l)$ then ${k^*}^l = k^*$, so for each element $c \in k$ there exists one and only one element $t \in k$ such that $t^l = c$, and so for each element $x \in k$ there exists one and only one element $y \in k$ such that $y^l = x(x^{l^n} - 1)$. This means that $N = q$, hence $N_1 = N + 1 = q + 1$. If $q \equiv 1(\bmod l)$ and $q \not\equiv 1(\bmod l^{n+1})$, then the greatest power of l dividing $q-1$ is of the form l^m with $1 \le m \le n$. The cyclic multiplicative group k^* is the internal direct product of its subgroups U_{l^m} of order l^m and $U_{\frac{q-1}{l^m}}$ of order $\frac{q-1}{l^m}$. Let χ be a character of k^* of order l, and let ρ be a generator of the group U_{l^m}. It holds

$$N = |\{(x,y) \in k \times k \mid y^l = x(x^{l^n} - 1)\}| = q + \sum_{r=1}^{l-1}\sum_{c\in k} \chi^r(c(c^{l^n} - 1)).$$

For $1 \le r \le l-1$ it holds

$$\sum_{c\in k}\chi^r(c(c^{l^n}-1)) = \sum_{d\in U_{\frac{q-1}{l^m}}}\sum_{j=0}^{l^m-1}\chi^r(d\rho^j(d^{l^n}\rho^{jl^n} - 1)) =$$

$$= \sum_{d\in U_{\frac{q-1}{l^m}}}\sum_{j=0}^{l^m-1}\chi^r(\rho^j d(d^{l^n}-1)) = [\sum_{j=0}^{l^m-1}\chi^r(\rho^j)]\cdot[\sum_{d\in U_{\frac{q-1}{l^m}}}\chi^r(d(d^{l^n}-1))] = 0,$$

since
$$\sum_{j=0}^{l^m-1}\chi^r(\rho^j)=0,$$
χ^r being a non-trivial character of the group U_{l^m}. It follows that $N=q$, and so $N_1=N+1=q+1$.

b) Let $q\equiv 1(\bmod l^{n+1})$, and let ψ be a character of k^* of order l^{n+1} such that $\psi(\xi)=\zeta_{l^{n+1}}$, ξ a generator of the cyclic multiplicative group k^*. By lemma 1 with $x_1=0$ and $B_1(x)=x^{l^n}-1$ it holds
$$N=|\{(x,y)\in k\times k \mid y^l=x(x^{l^n}-1)\}|=\frac{1}{l}\sum_{j=0}^{l-1}|\mathcal{A}_j|,$$
where $\mathcal{A}_j:=\{(x,y)\in k\times k \mid y^l=\xi^jB_1(\xi^jx^l)\}$, $j=1,\dots,l-1$. The $\mathcal{A}_j$'s are diagonal curves of the form:
$$y^l-\xi^{j(l^n+1)}x^{l^{n+1}}=-\xi^j.$$
It holds ([Da-Ha],[Li-Ni], p. 291, Theorem 6.34)
$$|\mathcal{A}_j|=q-\sum_{r=1}^{l^{n+1}-1}\sum_{s=1}^{l-1}\psi^r(\xi^{-jl^n})\psi^{sl^n}(-\xi^j)\iota(\psi^r,\psi^{sl^n})=$$
$$=q-\sum_{r=1}^{l^{n+1}-1}\sum_{s=1}^{l-1}\zeta_{l^{n+1}}^{-rjl^n+sjl^n}\psi^{sl^n}(-1)\iota(\psi^r,\psi^{sl^n})=$$
$$=q-\sum_{r=1}^{l^{n+1}-1}\sum_{s=1}^{l-1}\zeta_{l^{n+1}}^{jl^n(s-r)}\iota(\psi^r,\psi^{sl^n}),$$
since $\psi(-1)=1$. It follows that
$$\sum_{j=0}^{l-1}|\mathcal{A}_j|=lq-\sum_{j=0}^{l-1}\sum_{r=1}^{l^{n+1}-1}\sum_{s=1}^{l-1}\zeta_{l^{n+1}}^{jl^n(s-r)}\iota(\psi^r,\psi^{sl^n})=$$
$$=lq-\sum_{r=1}^{l^{n+1}-1}\sum_{s=1}^{l-1}\iota(\psi^r,\psi^{sl^n})\sum_{j=0}^{l-1}\zeta_{l^{n+1}}^{jl^n(s-r)}=$$
$$=lq-l\sum_{1\le r\le l^{n+1}-1,\,1\le s\le l-1,\,l|s-r}\iota(\psi^r,\psi^{sl^n}).$$
Therefore
$$N=\frac{1}{l}\sum_{j=0}^{l-1}|\mathcal{A}_j|=q-\sum_{1\le r\le l^{n+1}-1,\,1\le s\le l-1,\,l|s-r}\iota(\psi^r,\psi^{sl^n})=$$
$$=q-\sum_{s=1}^{l-1}\sum_{i=0}^{l^n-1}\iota(\psi^{s+il},\psi^{sl^n}).$$
The automorphisms σ of the abelian field extension $\mathbb{Q}(\zeta_{l^{n+1}})/\mathbb{Q}$ are given by $\zeta_{l^{n+1}}^{\sigma}:=\zeta_{l^{n+1}}^{s+il}$, $1\le s\le l-1$, $0\le i\le l^n-1$. It holds
$$\iota(\psi,\psi^{l^n})^{\sigma}=\iota(\psi^{s+il},\psi^{(s+il)l^n})=\iota(\psi^{s+il},\psi^{sl^n}),$$

hence

$$N = q - \sum_{s=1}^{l-1}\sum_{i=0}^{l^n-1} \iota(\psi^{s+il}, \psi^{sl^n}) = q - \sum_{\sigma\in \mathrm{Gal}(Q(\zeta_{l^{n+1}})/\mathbb{Q})} \iota(\psi, \psi^{l^n})^\sigma =$$

$$= q - \mathrm{Tr}_{\mathbb{Q}(\zeta_{l^{n+1}})/\mathbb{Q}}(\iota(\psi, \psi^{l^n})). \square$$

Proposition 2. *If* $q \equiv 1(\mod l^{n+1})$ *then*

$$L_{C_n}(t) = \prod_{\sigma\in \mathrm{Gal}(\mathbb{Q}(\zeta_{l^{n+1}})/\mathbb{Q})} (1 - \eta_n^\sigma t),$$

where $\eta_n := \iota(\psi^{l^n}, \psi)$, ψ *a character of order* l^{n+1} *of* k^*.

P r o o f: The L-polynomial of the curve C_n/k can be written in the form $L_{C_n}(t) = \prod_{j=1}^{2g_n}(1 - \alpha_j t)$, where $\alpha_1, \ldots, \alpha_{2g_n}$ are algebraic integers. For $r \geq 1$ it holds ([St], p.166, Theorem V.1.15.)

$$N_r = q^r + 1 - \sum_{j=1}^{2g_n} \alpha_j^r \tag{2}$$

Let ψ be a character of order l^{n+1} of the cyclic group k^*. The map

$$\psi_r : \mathbb{F}_{q^r}^* \to \mathbb{C}^*, \psi_r(x) := \psi(N_{\mathbb{F}_{q^r}|\mathbb{F}_q}(x))$$

is a character of order l^{n+1} of the cyclic group $\mathbb{F}_{q^r}^*$, and it holds ([Da-Ha],0.8)

$$\tau(\psi_r) = \tau(\psi)^r,$$

hence by (1)

$$\iota(\psi_r^{l^n}, \psi_r) = \frac{\tau(\psi_r^{l^n})\tau(\psi_r)}{\tau(\psi_r^{l^n+1})} = \frac{\tau(\psi^{l^n})^r\tau(\psi)^r}{\tau(\psi^{l^n+1})^r} = \iota(\psi^{l^n}, \psi)^r,$$

so by Proposition 1

$$N_r = q^r + 1 - \sum_{\sigma\in \mathrm{Gal}(\mathbb{Q}(\zeta_{l^{n+1}})/\mathbb{Q})} \iota(\psi_r^{l^n}, \psi_r)^\sigma =$$

$$= q^r + 1 - \sum_{\sigma\in \mathrm{Gal}(\mathbb{Q}(\zeta_{l^{n+1}})/\mathbb{Q})} (\iota(\psi^{l^n}, \psi)^\sigma)^r,$$

and so

$$\{\alpha_1, \ldots, \alpha_{2g_n}\} = \{\iota(\psi^{l^n}, \psi)^\sigma \mid \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{l^{n+1}})/\mathbb{Q})\}. \square$$

Let $m \geq 1$ be a natural number and let K be an algebraic number field with ring of integers $\mathcal{O}_K$ such that $\zeta_m \in \mathcal{O}_K$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ not dividing m, and let $x \in \mathcal{O}_K$ not divisible by $\mathfrak{p}$. The number $x^{\frac{N_{K/\mathbb{Q}}(\mathfrak{p})-1}{m}}$ is congruent modulo $\mathfrak{p}$ to one and only one root of unity $\zeta_m^l \in \mu_m$. The map

$$(\mathcal{O}_K/\mathfrak{p}) \setminus \{0\} \to \mu_m,\ x \bmod \mathfrak{p} \mapsto \zeta_m^l$$

is a character of order m of the multiplicative group of the finite field $\mathcal{O}_K/\mathfrak{p}$ called the *m-th power residue character modulo* $\mathfrak{p}$.

Proposition 3. *Let $\mathfrak{p}$ be a prime divisor of p in the ring $\mathbb{Z}[\zeta_{l^{n+1}}]$. Let ψ be the l^{n+1}-th power residue character modulo $\mathfrak{p}$. Identifying the finite field $\mathbb{F}_q$ with the residue class field $\mathbb{Z}[\zeta_{l^{n+1}}]/\mathfrak{p}$ it holds:*
a) The absolute value of the complex number $\iota(\psi^{l^n},\psi)$ is

$$|\iota(\psi^{l^n},\psi)| = \sqrt{q};$$

b) The prime ideal decomposition of the principal ideal generated by $\iota(\psi^{l^n},\psi)$ in the ring of integers $\mathbb{Z}[\zeta_{l^{n+1}}]$ is

$$\iota(\psi^{l^n},\psi)\mathbb{Z}[\zeta_{l^{n+1}}] = \mathfrak{p}^{\sum_{0\le u\le l^n-1, 1\le v\le l-1: ul+v(1+l^n)\le l^{n+1}} \sigma(u,v)^{-1}},$$

where $\sigma(u,v)$ is, for $0\le u\le l^n-1, 1\le v\le l-1$, the automorphism of $\mathbb{Q}(\zeta_{l^{n+1}})/\mathbb{Q}$ defined by $\zeta_{l^{n+1}}^{\sigma(u,v)} := \zeta_{l^{n+1}}^{ul+v}$.
c) In the ring $\mathbb{Z}[\zeta_{l^{n+1}}]$ it holds

$$\iota(\psi^{l^n},\psi) \equiv 1(\bmod\ (\zeta_{l^{n+1}}-1)^{l^n+1}).$$

The number $\iota(\psi^{l^n},\psi)\in\mathbb{Z}[\zeta_{l^{n+1}}]$ is uniquely determined by the properties a), b) and c).

P r o o f:
a): Every Jacobi sum in a finite field with q elements has absolute value $\sqrt{q}$.
b): By ([Ha1], p.40, (6.)) it holds

$$\iota(\psi^{l^n},\psi)\mathbb{Z}[\zeta_{l^{n+1}}] = \mathfrak{p}^{\sum_\sigma d(-l^n j_\sigma, -j_\sigma)\sigma},$$

where σ runs over the set of automorphisms of $\mathbb{Q}(\zeta_{l^{n+1}})$, j_σ mod l^{n+1} is defined by

$$\zeta_{l^{n+1}}^{\sigma^{-1}} = \zeta_{l^{n+1}}^{j_\sigma}$$

and

$$d(-l^n j_\sigma, -j_\sigma) = \begin{cases} 0 & \text{if } r(-l^n j_\sigma) + r(-j_\sigma) < l^{n+1} \\ 1 & \text{if } r(-l^n j_\sigma) + r(-j_\sigma) \ge l^{n+1} \end{cases},$$

$r(x)$ the smallest non-negative residue of x mod l^{n+1}. It holds

$$\sum_{\sigma\in \mathrm{Gal}(\mathbb{Q}(\zeta_{l^{n+1}})/\mathbb{Q})} d(-l^n j_\sigma, -j_\sigma)\sigma =$$

$$= \sum_{0\le u\le l^n-1, 1\le v\le l-1: r(-l^n(ul+v))+r(-ul-v)\ge l^{n+1}} \sigma(u,v)^{-1} =$$

$$= \sum_{0\le u\le l^n-1, 1\le v\le l-1: r(-l^n v)+r(-ul-v)\ge l^{n+1}} \sigma(u,v)^{-1} =$$

$$= \sum_{0\le u\le l^n-1, 1\le v\le l-1: l^{n+1}-l^n v+l^{n+1}-ul-v\ge l^{n+1}} \sigma(u,v)^{-1} =$$

$$= \sum_{0\le u\le l^n-1, 1\le v\le l-1: ul+v(1+l^n)\le l^{n+1}} \sigma(u,v)^{-1}.$$

c): For $c\in\mathbb{F}_q^*$ it holds

$$\psi(c) \equiv 1 \bmod (\zeta_{l^{n+1}}-1)$$

and

$$\psi^{l^n}(c) \equiv 1 \bmod (\zeta_{l^{n+1}}-1)^{l^n}.$$

Indeed, if $\psi(c) = \zeta_{l^{n+1}}^k$, $0 \le k < l^{n+1}$, then $\psi(c) - 1 = \zeta_{l^{n+1}}^k - 1$ is divisible by $\zeta_{l^{n+1}} - 1$ in $\mathbb{Z}[\zeta_{l^{n+1}}]$ and $\psi^{l^n}(c) - 1$ is divisible by $\zeta_{l^{n+1}}^{l^n} - 1$ which is associate with $(\zeta_{l^{n+1}} - 1)^{l^n}$. Then

$$\iota(\psi^{l^n}, \psi) = -\sum_{c \in \mathbb{F}_q} \psi^{l^n}(c)\psi(1-c) = -\sum_{c \in \mathbb{F}_q} \psi(c)\psi^{l^n}(1-c) =$$

$$= -\sum_{c \neq 1} \psi(c) - \sum_{c \neq 0,1} \psi(c)(\psi^{l^n}(1-c) - 1) =$$

$$= 1 - \sum_{c \neq 0,1} \psi(c)(\psi^{l^n}(1-c) - 1) \equiv$$

$$\equiv 1 - \sum_{c \neq 0,1} (\psi^{l^n}(1-c) - 1) \bmod (\zeta_{l^{n+1}} - 1)^{l^n+1} \equiv$$

$$\equiv 1 - \sum_{c \neq 0,1} \psi^{l^n}(1-c) + \sum_{c \neq 0,1} 1 \bmod (\zeta_{l^{n+1}} - 1)^{l^n+1} \equiv$$

$\equiv 1+1+q-2 \bmod (\zeta_{l^{n+1}} - 1)^{l^n+1} \equiv q \bmod (\zeta_{l^{n+1}} - 1)^{l^n+1} \equiv 1 \bmod (\zeta_{l^{n+1}} - 1)^{l^n+1}$. Two numbers in $\mathbb{Z}[\zeta_{l^{n+1}}]$ with the same absolute value and the same prime ideal decomposition differ by a root of unity. The only root of unity in $\mathbb{Z}[\zeta_{l^{n+1}}]$ which is $\equiv 1 \bmod (\zeta_{l^{n+1}} - 1)^{l^n+1}$ is 1. The properties a), b), c) determine the number $\iota(\psi^{l^n}, \psi)$ in $\mathbb{Z}[\zeta_{l^{n+1}}]$. $\square$

References

[Da-Ha] *Davenport, H., Hasse, H.*, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J.Reine Angew. Math. **172**(1934), 151-182. 5, 6

[Ha1] *Hasse, H.*, Zetafunktion und L-Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus, Abhandlungen der Deutschen Akademie der Wissenschaften Berlin, Math.-Nat. Kl. 1954, Nr. 4, 5-70. 7

[Li-Ni] *Lidl, R., Niederreiter, H.*, Finite Fields, Encyclopedia of Mathematics and Its Applications. 20. Cambridge: Cambridge Univ. Press, 1996. 5

[St] *Stichtenoth, H.*, Algebraic Function Fields and Codes, Springer, Berlin-Heidelberg, 1993. 6

Berlin and Bucharest

E-mail address: nicolae@math.tu-berlin.de